# Math 357
# Long quiz 05

2024–03–25 (M)

Your name: ____________________________________

Let $p = t^3 - 3t - 1 \in \mathbf{Q}[t]$.

(a) Prove that $p$ is irreducible.

(b) Prove that $p$ has three distinct zeros in $\mathbf{R}$. (You need not compute them.)

(c) Let $\alpha \in \mathbf{R}$ be a zero of $p$. Prove that $\sqrt{2} \notin \mathbf{Q}(\alpha)$.

**Solution:** Part (a): Because $p$ is a degree-3 polynomial over $\mathbf{Q}$, a field, $p$ is irreducible in $\mathbf{Q}[t]$ if and only if it has no zeros in $\mathbf{Q}$.[1] We may show that $p$ has no zeros in $\mathbf{Q}$ in various ways.

1. By the rational roots test,[2] if $\frac{r}{s} \in \mathbf{Q}$ is a zero of $p$ and in lowest terms, then $r$ divides the constant term of $p$ and $s$ divides the leading coefficient of $p$. This implies that if $\alpha \in \mathbf{Q}$ is a zero of $p$, then $\alpha = \pm 1$. Evaluating the function $p$ at these two values, we find

$$p(-1) = 1 \qquad\qquad p(1) = -3$$

so $p$ has no zeros in $\mathbf{Q}$, and hence is irreducible in $\mathbf{Q}[t]$.

2. Viewing $p \in \mathbf{Z}[t]$ and reducing its coefficients modulo 2, we get

$$\overline{p} = t^3 + t + 1$$

Evaluating $\overline{p}$ at the elements of the (finite) field $\mathbf{Z}/(2)$, we find

$$\overline{p}(0) = 1 \qquad\qquad \overline{p}(1) = 3 \equiv 1$$

so $p$ has no zeros in $\mathbf{Z}/(2)$, and hence is irreducible in $(\mathbf{Z}/(2))[t]$, hence in $\mathbf{Z}[t]$,[3] hence (by Gauß's lemma[4]) in $\mathbf{Q}[t]$.

3. Evaluating $p$ at $t+1$, we get

$$p(t+1) = t^3 + 3t^2 - 3$$

which by the Eisenstein–Schönemann criterion[5] with $p = 3$ is irreducible in $\mathbf{Z}[t]$ and hence (by Gauß's lemma) in $\mathbf{Q}[t]$.

Part (b): Evaluating $p$ at a few small values of $t \in \mathbf{Z}$, we find[6]

| $t$ | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $p(t)$ | $-3$ | $1$ | $-1$ | $-3$ | $1$ |

In particular, $p(t)$ changes sign three times as $t$ increases over the interval $[-2, 2]$. If we view the polynomial $p \in \mathbf{Q}[t]$ as a function $\mathbf{R} \to \mathbf{R}$, then the intermediate value theorem implies that $p$ has three zeros in $\mathbf{R}$.

Part (c): To begin, note that

[1] See DF3e, Proposition 9.10, p 308.
[2] See DF3e, Proposition 9.11, p 308.
[3] See DF3e, Proposition 9.12, p 309.
[4] See DF3e, Proposition 9.5, p 303.
[5] See DF3e, Proposition 9.13, p 309.
[6] In settings where we have access to graphing applications, we might use these to guide our search.

1. The minimal polynomial of $\alpha$ over $\mathbf{Q}$ is $p$, because $p$ is monic, irreducible, and $p(\alpha) = 0$.[7] Thus

$$[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg p = 3$$

2. The minimal polynomial of $\sqrt{2}$ over $\mathbf{Q}$ is $m_{\sqrt{2},\mathbf{Q}} = t^2 - 2$. Thus

$$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = \deg m_{\sqrt{2},\mathbf{Q}} = 2$$

Let $K : \mathbf{Q}$ be a field extension such that $\sqrt{2} \in K$. Then $\mathbf{Q}(\sqrt{2})$ is an intermediate field of $K : \mathbf{Q}$, so we get a tower of field extensions:

$$K : \mathbf{Q}(\sqrt{2}) : \mathbf{Q}$$

By the tower law, the degrees of these extensions satsify[8]

$$[K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$$

In particular, $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ divides $[K : \mathbf{Q}]$. That is, if $\sqrt{2} \in K$, then $2 \mid [K : \mathbf{Q}]$. Equivalently, if $2 \nmid [K : \mathbf{Q}]$, then $\sqrt{2} \notin K$. Because $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$ is not divisible by 2, we conclude that $\sqrt{2} \notin \mathbf{Q}(\alpha)$.

[7] See DF3e, Proposition 13.9, p 520, and the subsequent discussion.
[8] See DF3e, Theorem 13.14, p 523.